Reducing IoT Ecosystem exposure to breaches, data theft, and ruined reputations:

7 Key Elements for Proactive IoT Security

ICMC 2017

Loren Shade – Allegro Software

$10 Billion

27+ Million Medical Records Breached in 2016

ICMC17

Allegro

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

Mattel in hot water over interactive Hello Barbie

Mattel hopes to score big with Hello Barbie. Instead, the doll that records conversations and talks back is being branded as creepy and a spy.

Hello Barbie Doll Vulnerable to Hackers

by Robert Hackett @rhhackett DECEMBER 4, 2015, 8:43 PM EDT

Children's toy, or hacker's plaything?

Welcome to the Internet of toys.

Hello Barbie, Mattel's Internet-connected iconic doll, has a few insecurities. Computer security researchers dug into the toy's accompanying app and discovered several flaws that let hackers eavesdrop on communications between it and the cloud servers it connects to.

ICMC17 Allegro

IoT Security and the Enterprise

FORRESTER® RESEARCH

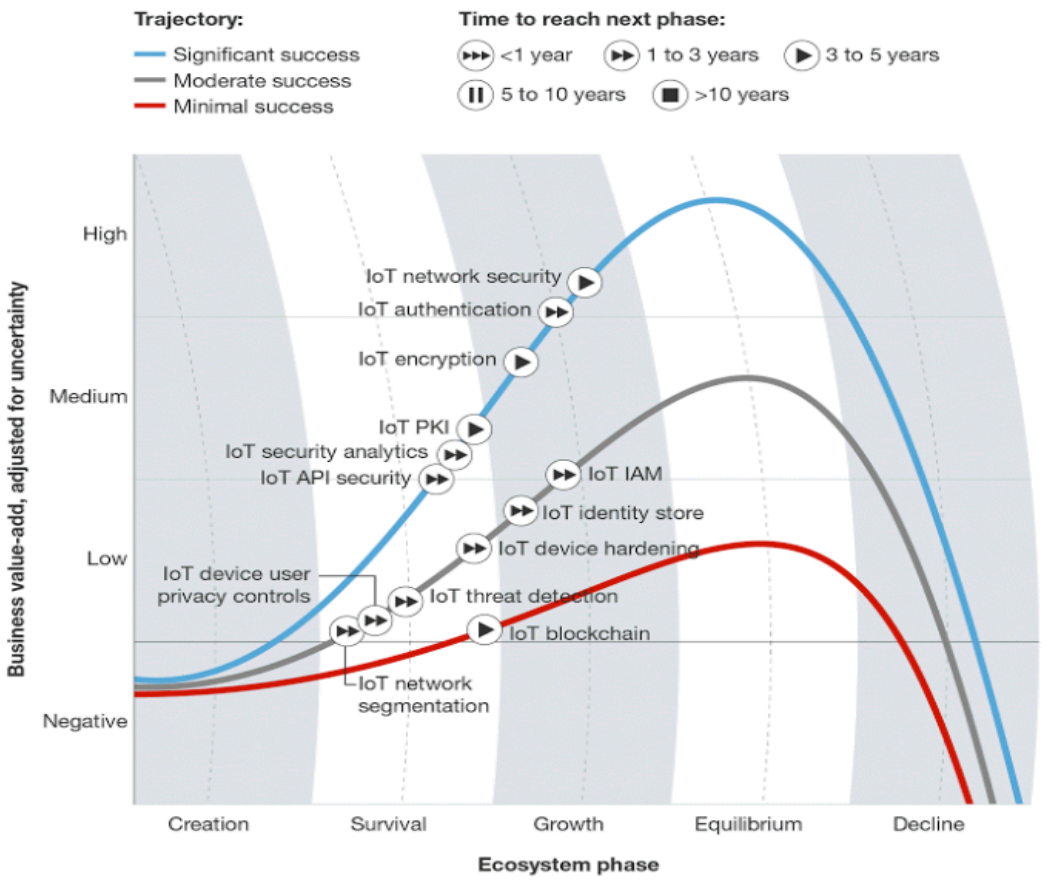
TechRadar™: Internet Of Things Security, Q1 '17

TechRadar™: Internet Of Things Security, Q1 2017

”IoT Manufacturers don’t care”

“…there is no single, magic security bullet that can easily fix all IoT security issues.”

https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#4157f0d61b49



117394 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

7 Key Elements of Proactive IoT Security

IoT Root of Trust

IoT ecosystems must be confident of the integrity and resulting data from all participating IoT devices.

ICMC17

Allegro

The Challenge: How to prevent identity theft, data corruption, and use of fraudulent hardware?

The Solution: Implement a method for establishing a root of trust during manufacture. When Public Key Infrastructure (PKI) technology is used, a Certificate Authority (CA) is required. GlobalSign and DigiCert are two vendors that provide commercial IoT CA implementations. Another popular but less secure option is to be your own private certificate authority.

The Benefits: Authentication, authorization, and validation of IoT devices into the larger IoT ecosystem significantly reduce risks associated with fraudulent data, hardware, data theft, loss of control, and much more.

Secure Parameter and Key Storage

Establishing and maintaining a root of trust for an IoT device relies on the ability to store and retrieve keys securely, along with operating and configuration parameters.

Technology	Risk	Specialized Hardware?	Description
On-Chip Secure Zone	Lowest	Yes	Various silicon vendors offer support for "trust zones" within the chip that are separate from the core processor, memory and bus structure. This approach offers the least risk to exposing critical data.
Trusted Platform Module (TPM)	Low	Yes	This is an additional item on the bill of materials. It is the favored technology by the Trusted Computing Group for storing critical data and establishing a root of trust.
Hardware Security Module (HSM)	Low	Yes	Similar to a TPM, HSMs also represent an additional item on the bill of materials and are typically optimized for specific cryptographic operations to offer overall performance.
Hybrid – NVRAM using Software TPM	Medium	No	The Trusted Computing Group also suggests solutions for software-based TPMs. While these are less secure than hardware modules, they offer tremendous flexibility and lower cost.
NVRAM using Cryptographic Routines	High	No	Similar to a software TPM, this implementation uses a simple hash or cipher with static keys. This can be secure as long as the keys are not discovered.
Keys stored as part of executable image	Highest	No	Unfortunately, this is the normal mode of operation for many IoT devices. Many vendors have seen their devices compromised and enrolled as unwitting servants of rogue DDOS botnets.

The Challenge: How to securely store operational parameters and keys on an IoT device that is often deployed in potentially harsh environments where keys can be compromised?

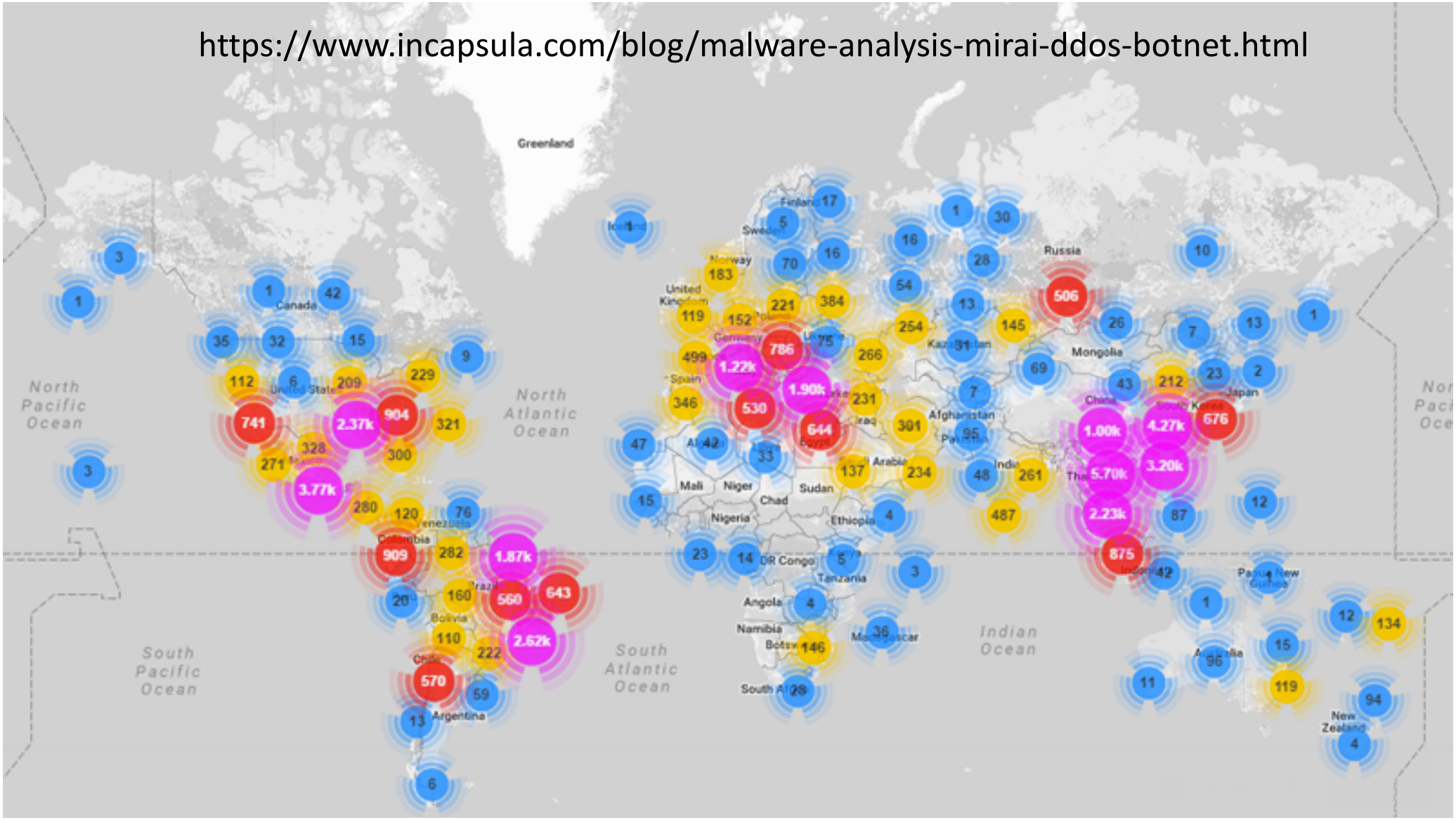
The Solution: Use industry-proven technologies for storing keys and critical operational parameters. On-Chip solutions offer the least risk, while storing keys in the code is not recommended.

The Benefits: Device identity is intact and the overall risk for malicious intent is dramatically reduced.

Secure Device Provisioning

The loss of identity and insecure re-provisioning of IoT devices have been identified as the root cause for many recent DDOS attacks worldwide.

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html



The Challenge: How to install and safely update firmware or operating parameters securely while the IoT device is deployed in operational environments?

The Solution: An engineered provisioning solution that uses digital signatures in combination with a secure multistage bootloader to implement firmware and parameter updates for devices deployed in the field.

The Benefits: A system designed to ensure secure updates provides an extremely valuable service to the end customer and dramatically reduces the risk of a rogue actor enrolling IoT devices in large-scale DDOS attacks.

Operational Data Security

Securing Data in Motion and at Rest


ENCRYPTION
DATA AT REST &
DATA IN MOTION


TLS

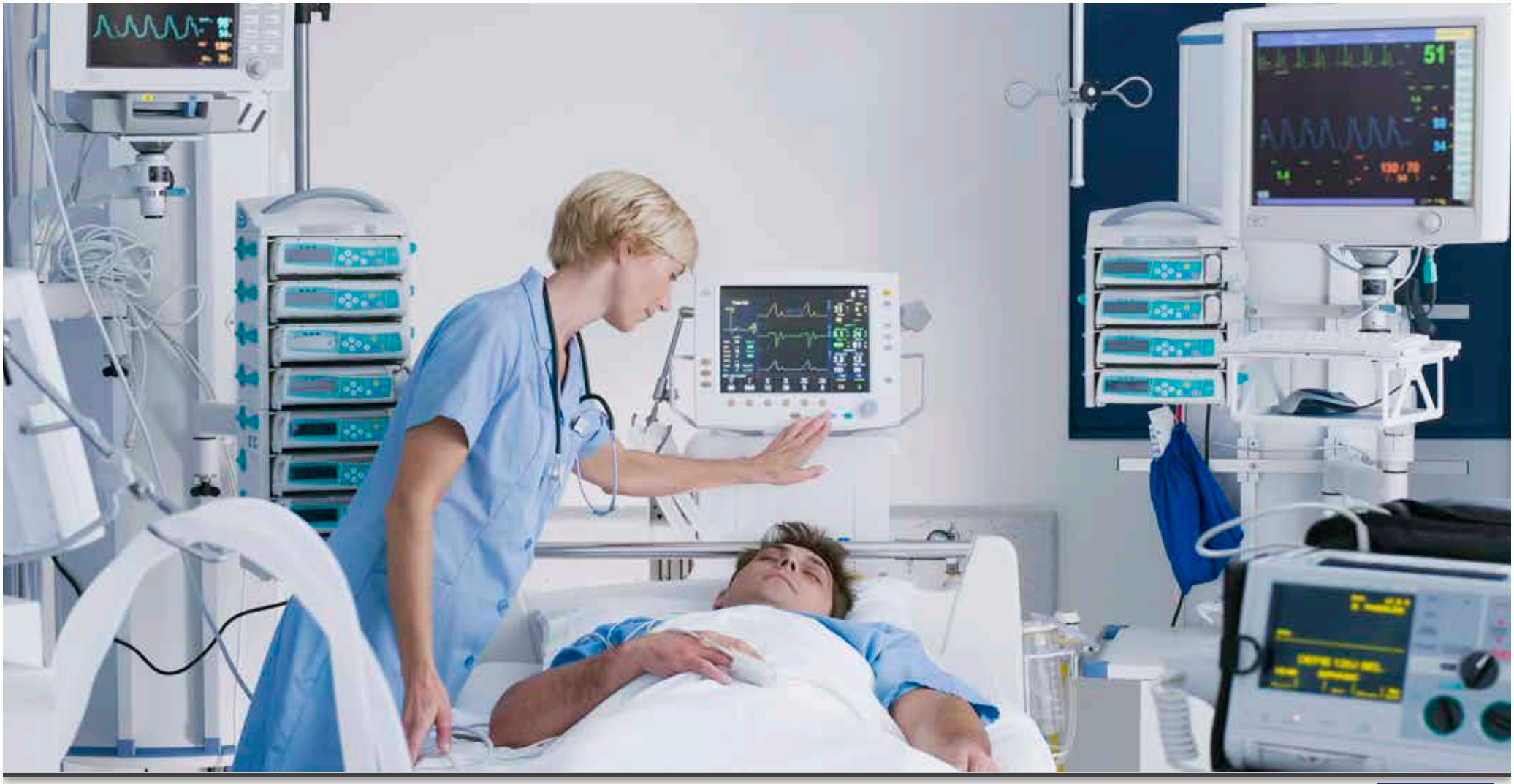
The Challenge: How to securely store and communicate generated IoT application data to the larger IoT ecosystem?

The Solution: Secure data-in-motion using the latest TLS protocols and secure data-at-rest using PKI technology.

The Benefits: All data exchanged between the IoT device and the larger IoT ecosystem is protected by TLS. If a breach occurs with a physical endpoint, data stored on the device is rendered useless.

Access Control and Key Management

The use of “factory defined” access credentials represent the largest single attack vector for IoT devices. The use of multiple keys and proper Key Management enable significant capabilities.



ICMC17

Allegro

The Challenge: How to manage IoT device keys, configuration, and user credentials securely?

The Solution: Use standards-based certificate management tools in partnership with an IoT-focused CA or custom implementation of a private CA with a robust infrastructure.

The Benefits: Implementation and effective use of certificates embeds multiple layers of security into an IoT device. This empowers developers with the ability to create mutually exclusive data stores to store critical data effectively and safely throughout the life cycle of the IoT device.

Monitor and Remediate

Monitoring and remediation provide a vital feedback function for an IoT ecosystem.

ICMC17 Allegro

The Challenge: How to monitor and remediate the deployed IoT devices to keep the ecosystem healthy?

The Solution: Implement a secure, flexible, and configurable IoT communications, command, and control architecture based on TLS, XML, RESTful APIs, or SOAP.

The Benefits: Strong monitorying leads to a healthy IoT ecosystem with secure IoT nodes actively reporting application data. Proactively identifying potential threats and inconsistencies prevents the disruption of the quality and overall health of the IoT ecosystem.

Validated Cryptography for IoT Devices

Cryptography is steeped in advanced math concepts and, to be useful, it must be tightly coupled with computer science and implementation skills. For resource-constrained IoT devices, an understanding and respect for the limits of embedded computing are mandatory.

ICMC17

Allegro

The Challenge: Does the cryptography used in my IoT device implement the cipher suites and complex algorithms correctly?

The Solution: Use validated cryptography – cryptographic solutions that have gone through independent third-party evaluation and extensive testing to ensure proper operation. Using validated cryptography also ensures interoperability and functionality with other deployed platforms.

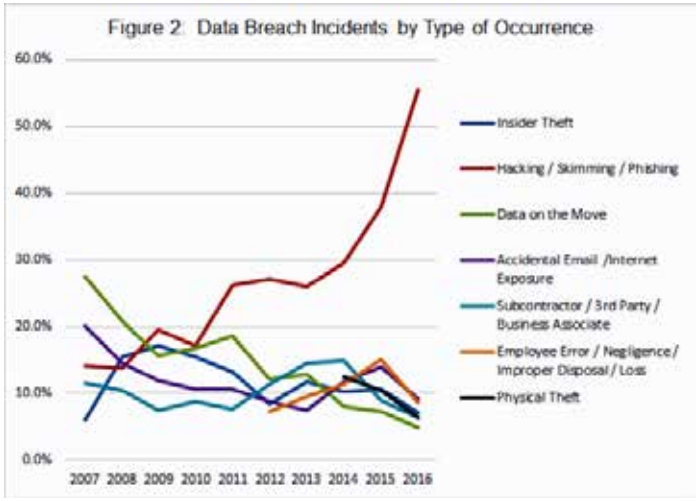
The Benefits: Using FIPS-validated cryptography leads to a high level of trust that the private data in IoT devices and their connected ecosystems remains private.

Environment: The Hospital

- System of Systems
  - Large Systems Integrator
    - Heterogeneous
  - Cost of not getting it right
    - Potentially life threatening
    - Potential legal ramifications
    - Potential financial implications
      - Lawsuits
      - Federal or civil penalties

HACKING Medical Records

- Data breach increase 40% for 2016
  - Healthcare : 34.5% of total
- Hacking accounts for over 50%
- IoMT/IoT NOT Immune
  - Miria, IRCTelnet, Aidra
  - LizardStresser, Lizkebab, Bashlite
  - Torlus, Gafgyt
  - Over 1 Million Miria infected IoT devices



Sources – ITRC, DataBreachToday

Why are IoMT Hacking Targets

- IoMT and Hospitals are:
  - Aggregators of Large Quantities of Personally Identifiable Information (PII)
  - Well equipped to save lives, ill equipped for cyber attacks
  - IoMT handle significant amounts of PII
  - Used as Pivot Point to Data

Sources – TechNewsWorld

Medical Record Breaches

- 27+ Million medical records breached in 2016
- Worth ~$500+ Million on the black market
  - Medical record worth $20-$40 compared to $5 for financial record
- ~$10+ Billion for Remediation
  - $402 average cost per stolen record

Sources – HHS,
Threatpost,
Ponemon Institute

ICMC17 Allegro

Thank You

Copy of the white paper, questions, or comments

TEXT iotsecurity to 44222

Or Visit

bit.ly/iotsecuritynow

goo.gl/NPLIqZ

loren@allegrosoft.com
978-264-6600